Amendments to the Claims: Please amend the claims as shown. Applicant reserves the right to pursue any canceled claims at a later date.

1.-23. (canceled)

24. (currently amended) A method for transmitting data, comprising:

providing each of a plurality of users of a communications network with a secret encryption program and a secret algorithm for generating an encryption key;

by a first user of ~~a~~ the communication network:

receiving a first random value originating from a first stochastic process;

generating a first symmetrical encryption key based on the first random value using the secret algorithm;

transmitting the first random value to a second user of the communication network;

by the second user:

receiving the first random value from the first user; and

generating the first symmetrical encryption key based on the received random value using the secret algorithm;

the first and second users then communicating encrypted data over the communications network using the secret encryption program and the first symmetrical encryption key; and

wherein the first random value comprises a digital value derived from a sensor output of an operational measurement of an automation system.

25-27. (canceled)

28. (previously presented) The method as claimed in claim 24, wherein the first stochastic process includes an operational time-variable parameter of an automation system.

29. (canceled)

30. (previously presented) The method as claimed in claim 24, further comprising:

by the second user:

receiving a second random value originating from a second stochastic process;

generating a second symmetrical encryption key based on the second random value;

transmitting the second random value to the first user;

by the first user:

receiving the second random value from the second user; and

generating the second symmetrical encryption key based on the received random value.

31-32. (canceled)

33. (currently amended) The method as claimed in claim 30, wherein one of the plurality of users is designated as a master user, and the first and second symmetrical encryption keys are generated by the plurality of users upon a request by ~~a~~ the master user of the communication network.

34. (previously presented) The method as claimed in claim 30, wherein the first and second symmetrical encryption keys are generated at predetermined times or after a lapse of a predetermined time interval.

35. (previously presented) The method as claimed in claim 24, wherein the first random value is transmitted over the communication network at a time of low utilization of the communication network.

36. (canceled)

37. (previously presented) The method as claimed in claim 24, wherein the first random value is transmitted using an asymmetrical encryption method.

38-39. (canceled)

40. (currently amended) A communication system, comprising:

at least first and second users; and

a communication network for transmitting data between the at least first and second users,

the first user comprising:

a first receiver for receiving a first random value originating from a stochastic process,

an encryption key generator for generating a first symmetrical encryption key based on the first random value,

a storage unit for storing the first symmetrical encryption key, and

a transmitter for transmitting the first random value to the second user via the network;

the second user comprising:

a first receiver for receiving the first random value from the first user, and

an encryption key generator for generating the first symmetrical encryption key based on the first random value received from the first user,

wherein data transferred between the users is encrypted and unencrypted via the first symmetrical encryption key; and

wherein the first random value comprises a digital value derived from a sensor output of an operational measurement of an automation system~~, with at least one high order bit of the digital value removed to reduce a periodic component of the operational measurement~~.

41. (currently amended) The communication system as claimed in claim 40, wherein the communication network is a public network, and wherein at least one high order bit of the digital value is removed to reduce a periodic component of the operational measurement.

42. (previously presented) The communication system as claimed in claim 40, wherein the second user further comprises:

a second receiver for receiving a second random value originating from a stochastic process, and

a transmitter for transmitting the second random value to the first user via the network,

the encryption key generator generates a second symmetrical encryption key based on the second random value, and

the storage unit stores the first and the second symmetrical encryption keys,

wherein the first user further comprises:

a second receiver for receiving the second random value from the second user,

the encryption key generator generates a second symmetrical encryption key based on the second random value, and

the storage unit stores the first and the second symmetrical encryption keys,

wherein data transferred between the users is encrypted and unencrypted via the symmetrical encryption keys.

43. (previously presented) The communication system as claimed in claim 42, wherein the communication network is the internet, and the first user is a master user for triggering the generating of the first and second symmetrical encryption keys by issuing a request via the internet.

44. (currently amended) The communication system as claimed in claim 42, wherein the communication network is an Ethernet, and the first or second user is a master user configured to output a command onto the Ethernet for triggering the generation of the first and second symmetrical encryption keys.

45. (currently amended) The method as claimed in claim 24, wherein the first random value is transmitted to ~~a~~ the plurality of users and the first symmetrical encryption key is generated at each of the plurality of users using the secret algorithm.

46. (previously presented) The method as claimed in claim 30, wherein the first symmetrical encryption key is used to encrypt data transmitted during a first time interval and the second symmetrical encryption value is used to encrypt data transmitted during a second time interval.

47. (currently amended) A method for transmitting data, comprising:

by a first user of a communication network:

storing a first random measured value received from a first stochastic process;

generating a first symmetrical encryption key based on the first random measured value;

transmitting the first measured random value to a second user of the communication network;

receiving ~~the~~ a second random measured value from the second user;

generating a second symmetrical encryption key based on the received random value;

by the second user:

storing the second random measured value received from a second stochastic process;

generating the second symmetrical encryption key based on the second random measured value;

transmitting the second ~~measured~~ random measured value to the first user;

receiving the first random measured value from the first user;

generating the first symmetrical encryption key based on the received ~~measured random~~ first random measured value,

wherein the first symmetrical encryption key is used to encrypt data transmitted between the first and second users during a first time interval, and the second symmetrical encryption ~~value~~ key is used to encrypt data transmitted between the first and second users during a second time interval; and

wherein the first and second random measured values each comprise a respective digital value derived from a respective different sensor indicating an operational measurement of an automation system~~, with at least one high order bit of each respective digital value removed to reduce a periodic component of the operational measurement~~.

48. (previously presented) The method as claimed in claim 47, wherein the first random value is an input to a function and an output of the function is used to generate the first symmetrical encryption key.

49. (previously presented) The method as claimed in claim 47, wherein the second random value is an input to a function and an output of the function is used to generate the second symmetrical encryption key.

50. (previously presented) The method as claimed in claim 24, wherein the first random value comprises a combination of at least two digital values obtained from respective different sensors indicating respective different operational measurements of an automation system.

51. (currently amended) The ~~communication system~~ method as claimed in claim 50, wherein the first random value comprises a concatenation of at least two digital values obtained from respective different sensors indicating respective different operational measurements of an automation system.